nesprávny výpočet ($x \notin L$): C_1, C_2, C_3 $l_1 = 2, l_2 = 3, l_3 = 4$

Definícia Logický obvod s n vstupmi $x_1, \ldots, x_m$ a 1 výstupom je orientovaný acyklický graf taký, že:

- v každom vrchole je buď niektore x_i (vrchol bez vstupných hrán) alebo AND, OR (vrchol s 2 vstupnými hranami) alebo NOT (vrchol s 1 vstupnou hranou), počet výstupných hrán je neobmedzený.
- jeden z vrcholov je výstupný

Definícia *Charakteristické* funkcia pre množinu $D \subseteq \{0,1\}^n$ je booleovská funkcia $f(x_1, \ldots, x_n$, taká, že $f(x_1, \ldots, x_n) = 1 \iff x_1, \ldots, x_n \in D$.

Veta Nech $L \in BPP$, $L \subseteq \{0,1\}^*$, Potom platia nasledovné dve tvrdenia:

1. Pre jazykk L existuje polynóm $p(x)$ a pravdepodobnostný polynomiálny algoritmus B s vlatnosťou:

   $$\forall n \exists y_n \in \{0,1\}^{p(n)} \text{ taký, že } \forall x \in \{0,1\}^n \text{ platí } :$$

   výpočet B na x s hodnotami *brand* určenými reťazcom y_n je správny (teda algoritmus B poznajúc y_n neurobí chybu na žiadnom vstupe $x \in \{0,1\}^n$.

2. Pre L existuje polynóm $q(n)$ taký, že $\forall n$ existuje logický obvod s n vstupmi, 1 výstupom a najviac $q(n)$ vrcholmi, ktorý počíta charakteristickú funkciu pre $L \cap \{0,1\}^n$.

Dôkaz Veta o vylepšovaní $\Longrightarrow$ existuje pravdepodobnostný algoritmus A akceptujúci L v nejakom polynomiálnom čae $s(n)$ s chybou $\frac{1}{7}$ ($= \Sigma'$).

Dôsledok (dôkazu) Existuje pravdepodobnostný algoritmus A', ktorý v čase $O(nS(n))$ akceptuje slová patriace do $L \cap \{0,1\}^n$ s chybou $\frac{1}{2}(s(1-\frac{1}{7})\frac{1}{7})^{n+\frac{1}{2}} = \frac{1}{2}\left(\frac{24}{49}\right)^{n+\frac{1}{2}} < \left(\frac{1}{2}\right)^{n+\frac{3}{2}} \forall n$.

Fakt Nech $C_1, \ldots, C_r$ sú všetky nesprávne výpočty A' na x s počtom $l_1, \ldots, l_r$ volaní procedúry *brand*. Potom $\sum_{i=1}^{r} 2^{-l_i}$ = pravdepodobnosť chyby A' na x (lebo A' vykoná c_i s pravdepodobnosťou 2^{-l_i}.

Upravme A' tak, aby po zistení výsledku (akceptuj/zamietni) vykonal na x dĺžky n ešte toľko volaní *brand*, aby ich celkový počet bol $(2n+1)s(n)$. Nech A'' označuje upravený A'.

$\forall x \in \{0,1\}^n : Y_x^n = \{y \in \{0,1\}^{(2n+1)s(n)}|$výpočet A' na x určený reťazcom y je nesprávny$\}$

$|Y_x^n|$ = počet nesprávnych výpočtov na A'' na x je $\sim_{i=1}^{r} 2^{(2n-1)s(n)-l_i} = 2^{(2n+1)s(n)}$ (pravdepodobnosť chyby A'' na x) $\leq$ (*) $2^{(2n+1)s(n)} \cdot (\frac{1}{2})^{n+\frac{3}{2})}$ (**).

$$|Z^n| \geq - \sum_{x \in \{0,1\}^n} |Y_x^n| \geq (**) 2^{(2n+1)s(n)} (1 - 2^n (\frac{1}{2}^{n+\frac{3}{2}})$$

$$= 2^{(2n+1)s(n)(\underbrace{\geq \frac{1}{2}} 1-(\frac{1}{2}^{\frac{3}{2}})} \geq 1$$

$$\implies Z^n \neq \emptyset \implies \forall n \exists y_n \implies$$

výpočet A'' na x určený reťazcom y_n je správny $\forall s \in \{0,1\}^n \implies$ (a) platí pre $B = A''$ a $p(n) = (2n+1)s(n)$.

Dôkaz (2) Idea: Logický obvod počítajúci charakteristickoú funkciu pre $l \cap \{0,1\}^n$ zostrojíme tak, aby simuloval výpočty agoritmu B (pre jednoduchosť deterministický Turingov stroj M simulujúceho B) na $x \in \{0,1\}^n$ určené reťazcom y_n.

```
              |<---n--->|
|cent|    x      |#|    y_n    | ...
                 ^

        |
        q  M = (\Sigma, Q, q_, \delta, F)
```

Obr. 1: T-Stroj M

Štruktúra obvodu: (chýba obrázok)

$\forall i, j D_{i,j}$ má na vstupe binárne kódované nasledovné informácie pre j-ty krok výpočtu stroja M:

- obsaho i-teho políčka ($\lceil \log |\Sigma| \rceil$ bitov).
- či je i-te políčko čítané (1 bit)
- stav $q \in Q$ (ak je i-te políčko čítané ($\lceil \log |Q| \rceil$ bitov).
- pohyb hlavy (ak je i-te políčko čítané) 1/0/-1 (2 bity)

Bloky $D_{i,j}$ majú $3k$ bitov na vstupe a k bitov na výstupe. Každý blok $D_{i,j}$ treba nahradiť pomocou k logických obvodov s $3k$ vstupmi a 1 výstupom. Výsledný logický obvod počíta charakteristickú funkciu pre $L \cap \{0,1\}^n$ a má polynomiálne veľa vrcholov.

```
procedure Freivalds (A,B,C,r) {
// overí rovnosť AB=C s pravdepodobnosťou omylu $2^{-r}$
// A,B,C sú matice rádu $n*n$
náhodne vyber bin. bektory z_1, z_2, \ldots z_r dĺžky n
if (z_i, A)B = z_i C \forall i then return "yes"  (s pravdepodobnosťou omylu
\leq 2^{-r})
```

```
else return "no" (bez omylu)
}
```

Časová zložitosť $O(rn^2)$.